Civilian Cybersecurity at LLNL

LLNL's Civilian Cyber Program is focused on enhancing the security and resilience of the nation's critical infrastructure systems and networks to cyber hazards.

Countering Cyber Threats

National security depends on safe and reliable operation of information technology (IT) and operational technology (OT) systems and networks. While information theft and financial profit have been the main objectives of cyberattacks, another concerning trend has emerged in the last several years. Cyberattacks on critical infrastructure such as dams, power plants, and power grids with intent to cause physical damage are on the rise. Today, federal networks and agencies are under constant cyberattack.

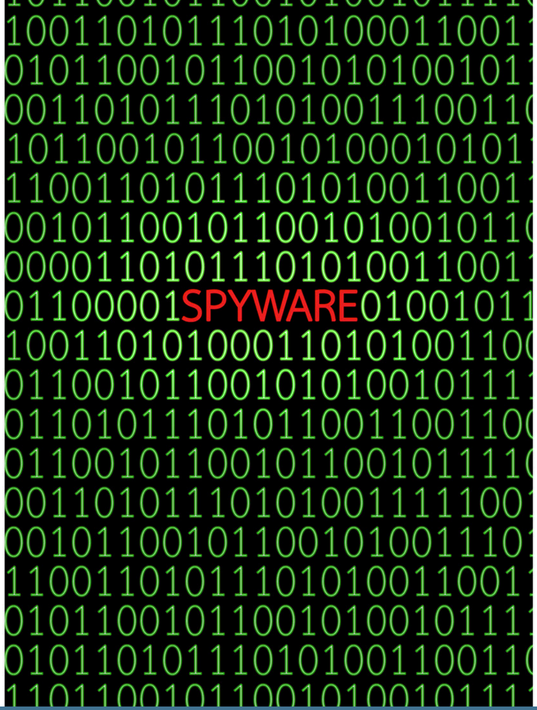
Lawrence Livermore National Laboratory (LLNL) brings its expertise in defending its own systems from cyberattack, and its knowledge and of the nature of cyber threats facing the nation through the work it has performed in a more than 20-year partnership with the intelligence community to civilian cyberdefense.

LLNL's civilian cyber program leverages our core competencies to support cyber security efforts in the Department of Homeland Security, Department of Energy, state and local governments, and industry to enhance the resiliency of government websites and that of critical infrastructure.

Accomplishments

Lawrence Livermore National Laboratory has established a research program to take on cybersecurity threats to the nation's critical infrastructure, including its energy systems and computer networks.

- As part of California Energy Systems for the 21st Century, Livermore explores next-generation cybersecurity of industrial control systems. Program focus is on machine-to-machine automated threat response (MMATR) to protect electricity grid infrastructure from cyberattacks. Livermore has developed a modeling and simulation platform, ParGrid, to evaluate consequences of cyber threats to California's transmission grid and test the performance of MMATR technologies.
- In the Grid Modernization Lab Consortium 1.4.23 project, the Laboratory's expertise in computational science and machine learning is being applied to provide smart meter data for detecting anomalies on the electricity grid. Machine learning has the potential to rapidly detect incursions.
- LLNL investigated the potential impacts of active scanning on energy delivery systems networks (EDS) and developed tools used on testbed equipment in the Safe Active Scanning for Energy Delivery Systems project. These tools allow users to test active scans from common, benign scans to extremely aggressive scans in realistic, production-like environments that impose significant burdens on EDS devices.
- Skyfall is a Livermore-developed EDS testbed representative of a common utility substation to test for vulnerability and grid-level impact analysis, firmware analysis, and malware analysis. Skyfall is connected to ParGrid, LLNL's coupled power transmission and communication model.
- Researchers in the Robust DERMS Control Verification project are working to enable distributed energy resource management systems (DERMS) for verifying that commands sent by a central authority will not damage the distribution system. The verification protects them from adversaries who gain control of the central command system's communications channel.
- QIARA (Quantitative Intelligent Adversary Risk Assessment) develops methods to quantify risk of cyberattack and understand the value of mitigation options.
- The CyTRICS project uses Livermore's automated software assurance tool ROSE to examine the software and firmware of devices on the grid to ensure their integrity against cyberattack.



Scientific Underpinnings

LLNL applies its skills, facilities, and computational tools developed for its national security work to address cyberthreats to the security and resiliency of civilian networks, operational systems, and critical infrastructure. LLNL's Civilian Cyber Program uses core competencies in high-performance computing (HPC), data analytics to handle the output from HPC simulations, and threat awareness (based on the Laboratory's longstanding relationship with the intelligence community). The Laboratory draws on the following key capabilities enabled by our core competencies:

- **Modeling and Simulation of Cyber-Physical Systems:** HPC enables development of high-fidelity, large-scale coupled, physics-based models of cyber and cyber-physical systems to understand effects, vulnerabilities, large-scale impacts, and mitigations.
- **Machine Learning and Data Analytics for Cyber Threat Detection:** The Laboratory uses its capabilities in machine learning and data analytics to develop systems that discern the difference between normal and off-normal behavior in physical systems and network traffic.
- **Collaborative Autonomy for Cyber Systems Resilience:** Collaborative autonomy entails the use of autonomous computing devices with algorithms that can communicate, pool data, operate through compromise, and make decisions collaboratively based on objective criteria about how to respond. Livermore is pioneering this technology, using systems as autonomous agents to search for, detect and counter cyberattacks in such infrastructure as computer network, power grids, transportation systems and industrial facilities.
- **Software Assurance:** Livermore's researchers develop automated tools to deconstruct software and trace execution pathways to identify intentional and unintentional vulnerabilities and inefficiencies in code. Using machine learning and Livermore-developed software, researchers can ensure the validity of software updates, and understand the origin of code, across software libraries.
- **Network Characterization and Security:** LLNL scientists combine active and passive techniques to gather and interpret network information to identify components, enumerate assets, and understand their configuration and network topology.
- **Cyber Risk and Resilience:** The Laboratory's experts provide quantitative estimates of risk from intelligent adversary threats and develop appropriate mitigation options using science-based, threat-informed methods.

The Future

LLNL's Civilian Cyber Program supports a wide range of customers—including the Department of Homeland Security, Department of Energy, state and local governments, and industry—to enhance cyber security and resiliency of .gov domain and critical infrastructure.

The program is expanding to address threats to the nation's network and IT infrastructure from hackers, organized criminal agents, and nation-state actors. The program is pushing toward a layered defense with three significant thrusts:

1) build hardware systems as securely as possible to defend against low-capability actors

2) develop technology to detect and respond to cyberattack in real time

3) develop technologies for resilient systems that can continue to operate while under cyberattack. This three-level defensive strategy is designed to counter a wide spectrum of credible threats from actors with varying levels of capability.

Principal Sponsorship

- DOE/NNSA, DHS, DOD, DOE/IN, and U.S. intelligence agencies

LLNL-MI-768187
This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.
February 21, 2019